

REMARKS

This Amendment is in response to the Office Action dated June 22, 2004. Claims 1-36 are pending in the present application. Claims 1-36 are rejected. Claims 1, 6, 7, 12, 13, 18, 25, 30 and 31 and 28 have been amended. Claims 4, 5, 16, 17, 28 and 29 have been cancelled. Accordingly, claims 1-3, 6-15, 18-27 and 30-36 remain pending in the present application.

Present Invention

A method and system for enabling an image to be authenticated is disclosed. The method and system comprises providing a digital signature associated with a device; and allowing a user to capture the image utilizing the device. The method and system further includes associating the digital signature and information related to the user with the captured image wherein the digital signature and the information related to the user are capable of being utilized to authenticate the captured image. The information related to the user comprises the user's identity. The method and system further includes utilizing a radio frequency interface to associate the user's identity with the captured image.

Claim Rejections – 35 USC 103

The Examiner states,

Claims 1-4, 13-16, 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman (USP 5,499,294) in view of Squilla et al., hereinafter Squilla (USP 5,898,779).

Friedman is silent in expressly disclosing that user related information is associated to the digital signature. Friedman's system only associates a digital image with a particular digital camera. It would be advantageous if the user who took the digital image could also be associated with the digital image. Squilla teaches a photograph's information may be included for subsequent authentication along with the

image and that the photographer's information is stored within the image hash in the digital signature (col. 5, line 60—col. 6, line 5).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Squilla within the system of Friedman because it would allow the system to be able to authenticate a digital image with both the camera that was used to take the image and the person who took the image.

As per claims 2, 14 and 26, Friedman teaches the device is capable of electronically transmitting images (col. 8, lined 30-33).

As per claims 3, 15, and 27, Friedman teaches the device comprises a digital camera (col. 8, line 30).

As per claims 4, 16, and 28, the examiner supplies the same rational for the motivation as recited in the rejection of claims 1, 13, and 25. Squilla teaches the information related to the user comprises the user's identity (col. 5, lines 64-65).

Claims 5-12, 17-24, and 29-36 are rejected under 35 U.S.C. 103(as) as being unpatentable over Friedman and Squilla as applied to claims 1-4, 13-16, 25-28 above, and further in view of Steinberg et al., hereinafter Steinberg (USP 5,862,217).

As per claims 5, 17, and 29, Friedman and Squilla are silent in disclosing utilizing a radio frequency interface to associate the user's identity with the captured image. Steinberg teaches utilizing a radio frequency interface to associate the user's identity with the captured image (col. 2, line 65—col. 3, line 7). This method provides an easy way for the user to input his/her information on a computer and have it downloaded to the digital camera. In view of this, it would have been obvious to one of ordinary skill in art at the time of the invention to employ the teachings of Steinberg within the combined system of Friedman and Squilla because it would allow the user to easily input his/her information on a computer where it could be downloaded to the digital camera.

As per claims 6, 18 and 30, Friedman teaches the user of a public and private key associated with a digital camera. Friedman does not disclose a public/private key pair associated with the user. Steinberg teaches a public/private key pair associated with the user (col. 4, lines 10-15). Steinberg uses a public/private key pair because of its proven ability to securely encrypt and decrypt confidential data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Steinberg within the combined system of Friedman and Squilla because it would provide a provable manner in which only a user who possessed the private key could have signed the digital image.

As per claim 7, 19, and 31, the examiner supplies similar rationale for the motivation as recited in the rejection of claims 5, 17, and 29 to incorporate the teachings of Steinberg within the system of Friedman and Squilla. Steinberg teaches utilizing a smart card to associate the user's identity with the captured image (col. 2, lines 57-58) for the same reason as mentioned above.

As per claims 8, 20 and 34, Friedman teaches the user of a public and private key associated with a digital camera. Friedman does not disclose a public/private key pair associated with the user. Steinberg teaches a public/private key pair associated with the user (col. 4, lines 10-15). Steinberg uses a public/private key pair because of its proven ability to securely encrypt and decrypt confidential data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Steinberg within the combined system of Friedman and Aquilla because it would provide a provable manner in which only a user who possessed the private key could have signed the digital image.

As per claims 9, 10, 21, 22, 33, and 34, Friedman teaches associated a private key with the captured image (col. 5, lines 55-58).

As per claims 11, 12, 23, 24, 35 and 36, Friedman teaches storing the captured image and the digital signature in a file, wherein the file is located within a memory of the digital camera; hashing the file thereby producing a digest; and associating the digest with the private key (col. 5, lines 55-65).

Applicant respectfully traverses this rejection. Applicant has amended independent Claims 1, 13 and 25 to include the limitations of claims 4 and 5, claims 16 and 17 and claims 28 and 29, applicant respectively submits that cited references neither teach nor suggest either singly or in combination the invention as recited in the independent claims.

Independent Claims 1, 13, and 26 have been amended to include utilizing a radio frequency interface to associate the user's identity with the captured image. Applicant agrees with the Examiner that Friedman and Squilla are silent in disclosing this recitation. Applicant further submits that although Steinberg discloses that "radiated signals can also be used for communication as indicated by transceivers 28-30" at column 2, lines 57-59. Steinberg nowhere teaches or suggests that utilizing a radio frequency interface to associate the user's identity with the captured image as recited in the claims. Steinberg discloses at column 2, line 65-column 3, line 7, supplying a password to the camera utilizing a variety of communication methods. Accordingly, the combination of

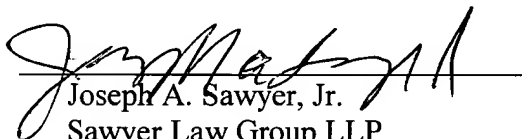
Steinberg with the other cited references would disclose a digital camera which includes a method for downloading a password for authentication. This is clearly different from the invention as recited in the independent claims.

Accordingly, the cited references neither teach or suggest either singly or in combination, the invention as recited in independent Claims 1, 13 and 25. Furthermore, claims 2, 3, 6-12, 14, 15, 18-24, 26, 27 and 30-36 are allowable since they depend from allowable base claims.

In view of the foregoing, Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

September 22, 2004


Joseph A. Sawyer, Jr.
Sawyer Law Group LLP
Attorney for Applicant
Reg. No. 30,801
(650) 493-4540